REMARKS

Claims 1-8 and 11-15 are pending in this application. Claim 12 has been amended to correct a typographical error. No new matter has been added.

The Examiner noted that in the claim sheet presented on November 13, 2007, claim 8 was identified as an amended claim, but there was no indication in the text of the claim of any changes. Claim 8 should have been identified as "Previously Presented." Applicants' representative thanks the Examiner for bringing this matter to his attention and apologizes for any inconvenience.

Rejections Under 35 U.S.C. § 112

Claim 1 was rejected under 35 U.S.C. § 112, second paragraph, because the terms “first manipulation means” and “means of instructions” were allegedly "not defined by the claims, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention." Claim 12 was similarly rejected under the rationale given above for "first manipulation means." Applicants respectfully traverse these rejections.

The “first manipulation means” and “means of instructions” in claims 1 and 12 are intended to invoke another section of 35 U.S.C. § 112, namely the sixth paragraph, which states "[a]n element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof."

Applicants respectfully submit that a person of ordinary skill in the art would

be reasonably apprised of the scope of Applicants' claimed subject matter by reviewing the corresponding structure, material, or acts described in the specification.

For example, support for the claimed "first manipulation means for supplying an output data item from an input data item" may be found, for example, on page 15, line 8 through page 17, line 10, in the discussion of the SBOX operation. Applicants' specification explains that the SBOX operation comprises a table of constants for supplying an output data item as a function of an input data item.

Support for the claimed "output data item is manipulated by means of instructions" may be found, for example, on page 8, lines 7-10. Applicants' specification explains that the instructions referred to are those that manipulate a target bit in a differential power analysis. Further descriptions of the instructions referred to can be found in the specification, for example, at page 17, lines 11-15, and page 18, lines 28-30.

Thus, upon reviewing the specification as a whole, a person of ordinary skill in the art would be readily apprised of the structure, material, or acts described in the specification that correspond with the claimed “first manipulation means” and “means of instructions.” Accordingly, the rejections under 35 U.S.C. § 112, second paragraph, should be withdrawn.

Rejections Under 35 U.S.C. § 103

Claims 1-8 and 11-15 were rejected under 35 U.S.C. § 103(a) as unpatentable over Kocher U.S. Patent No. 5,278,783 and Luyster U.S. Patent No. 6,182,216. Applicants respectfully traverse this rejection.

Applicants' claimed subject matter provides a counter measure against attacks on the security of cryptographic information by introducing randomness into the operations that are performed during the execution of the cryptographic algorithm. Referring to Applicants' Figure 3, one of the standard operations that is performed in each round of the DES algorithm is known as the SBOX operation, in which a 48-bit input value is converted into a 32-bit output value. This conversion is implemented by means of a table, an example of which is illustrated in Figure 6 of the application. Typically, the same table is employed in each of the 16 rounds of the DES algorithm.

In accordance with the claimed subject matter, a countermeasure is provided by using different tables during different rounds of the algorithm. After one table is established for the algorithm, another table is generated by performing an exclusive-OR operation on components of the first table, using a random value. As illustrated in the exemplary embodiment of Figure 7, one of the tables (TC_1) is used for some of the rounds of the algorithm, and the other table (TC_2) is used during other rounds of the algorithm.

Applicants respectfully submit that neither Kocher nor Luyster discloses, or otherwise suggests, such a technique as a countermeasure against attack on the security of cryptographic information.

For example, Applicants' claim1 recites a countermeasure method, wherein at least some of the rounds of a cryptographic algorithm are implemented with a first manipulating means that supplies an output data item from an input data item. In rejecting claim 1, the Action refers Kocher, at col. 6, lines 39-42. This cited passage describes the manner in which the permutations and blinded values for the cryptographic key K are produced. However, this cited passage lacks the specificity

needed to support a proper rejection. For example, Applicants have not been informed as to what feature disclosed in this passage is considered to constitute the claimed manipulating means that provides an output data item from an input data item. If the rejection based on Kocher is not withdrawn, the Examiner is respectfully requested to identify, with particularity, what feature in the patent is being interpreted as the first manipulating means

Claim 1 goes on to recite that at least one other round of the cryptographic algorithm is implemented with other manipulation means for supplying output data, wherein the other manipulation means are obtained from the first manipulation means by performing an exclusive-OR operation with a random value. Thus, the second, or "other," manipulation means is derived from the first manipulation means, by performing an exclusive-OR operation on it. The Action admits that Kocher fails to disclose this feature and turns to Luyster for support.

As an initial matter, since it is not apparent what feature described in Kocher is considered to correspond to the claimed first manipulating means, it is also not apparent how the Examiner proposes to combine Kocher and Luyster in order to arrive at the other manipulating means that is derived from the first manipulating means by performing an exclusive-OR operation with a random value.

Additionally, and regardless of Kocher's disclosure, Applicants respectfully submit that the cited section in Luyster neither discloses, or otherwise suggests, the claimed "other manipulation means for supplying output data, so that the output data item is unpredictable, said other manipulation means being obtained from said first manipulation means by performing an exclusive OR operation on said first manipulation means with a random value." For example, the cited sections in Luyster (col. 6, lines 39-53 and Fig. 6, block 124) are directed to the Khufu and

Khafre ciphers and the use of rotation to move bits. Here, too, Applicants have not been informed as to what feature disclosed in this passage is considered to constitute the claimed other manipulation means being obtained from the first manipulation means by performing an exclusive OR operation on the first manipulation means with a random value. If the rejection based on Luyster is not withdrawn, the Examiner is respectfully requested to identify, with particularity, what feature in the patent is being interpreted as the other manipulation means, and where Luyster discloses obtaining another manipulating means by performing an exclusive-OR operation on the first manipulating means.

Claim 1 recites that at least one of the multiple rounds of the cryptographic algorithm is implemented with the first manipulating means, and at least one other round of the algorithm is implemented with the other manipulation means. Hence, the claim explicitly recites that different manipulation means are employed in different respective rounds of the algorithm. It is respectfully submitted that even the combination of Kocher and Luyster does not disclose this subject matter. With respect to Kocher, it appears that the same blinded values are employed throughout the entire DES algorithm. There is no disclosure that suggests employing different operations during different respective rounds of the algorithm.

For at least these reasons, therefore, it is respectfully submitted that claim 1 is not obvious in view of Kocher and Luyster. For these same reasons, claim 12 is likewise patentably distinct from the references. Furthermore, since all other claims depend, directly or indirectly, from either claim 1 or claim 12, they are likewise not obvious in view of Kocher and Luyster.

Conclusion

For the foregoing reasons, Applicants respectfully submit that this application is in immediate condition for allowance and all pending claims are patentably distinct from the cited references. Reconsideration and allowance of all pending claims are respectfully requested.

In the event that there are any questions about this application, the Examiner is requested to telephone Applicants' undersigned representative so that prosecution of the application may be expedited.

If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: July 7, 2008

By: /Brian N. Fletcher/
Brian N. Fletcher
Registration No. 51,683

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620